社会科学进展
2025 年 1 月第 7 卷第 1 期

三亚市个人数据跨境流动安全防控的对策与建议

韦海浪

三亚学院，三亚

摘　要 | 自党的十八大以来，习近平总书记在多个会议中强调，“要切实保障国家数据安全”。随着数据量激增和数据跨境流动日益频繁，有力的数据安全防护和流动监管将成为国家安全的重要保障。海南省坚持不懈深入学习贯彻习近平总书记关于国家数据安全的重要论述精神，全面统筹推进各领域数据安全工作。三亚市积极响应国家政策和法规要求，明确表示未来三亚市将更加注重“保障国家数据安全，加强个人信息保护”。文章从个人数据跨境流动安全防控入手，既分析了三亚市个人数据跨境流动安全防控中存在的不足，又借鉴上海市、广州市的经验做法，提出四条建议，以完善三亚市个人数据跨境流动的安全防控措施。

关键词 | 个人数据；数据跨境流动；数据分类分级；监管；评估

1　三亚市个人数据跨境流动存在的安全风险

（1）个人数据泄露风险

作为旅游胜地，三亚市吸引了大量游客，这些游客的个人数据如身份信息、联系方式、住宿记录等，若被不当处理或者存储，极易引发泄露。如2021年8月11日，海南省互联网信息办公室通报了7款App违法违规收集使用个人信息情况，其中包括由三亚市天涯行城市通卡科技有限公司运营的“天涯行APP”，存在诸如未公开收集使用规则、未明确告知收集目的，以及缺乏有效的个人信息更正、删除及账号注销功能等问题。作为全国第五批跨境电子商务综合试验区的核心城市，三亚市正通过各种形式鼓励跨境电商的发展，如印发了《三亚市跨境电子商务专项资金暂行管理办法》《三亚市鼓励跨境电商发展措施实施细则》等文件。2023年11月22日，三亚跨境电商综试区线上综合服务平台正式上线，但在跨境电商活动中个人数据泄露问题依然存在，跨境电商平台需处理大量敏感信息，如信用卡信息和个人身份信息等，这些信息可能被黑客和网络犯罪分子窃取或滥用，进而导致用户的个人信息被滥用以及金融损失。同时，企业、机构以及政府部门在收集、处理个人数据时，若采取安全措施失当，也存在数据泄露的风险。

（2）个人数据分类模糊

但三亚市尚未有符合本市市情的个人数据分类标准，这在一定程度上抑制个人数据跨境流动。除此之外，需要进一步考虑以下问题：除了在三亚市产生的个人数据之外，对未在三亚市收集产生的个人数据如何跨境处理？“不在三亚市收集”如何认识理解？“收集行为不在三亚市”“主体的地理位置未在三亚市”还是“收集动作以及主体皆不在三亚市”？对未在三亚市收集产生但在境内进行加工处理的个人数据如何认定？如

作者简介：韦海浪，三亚学院法学院教师，研究方向：民商法。
文章引用：韦海浪. 三亚市个人数据跨境流动安全防控的对策与建议［J］. 社会科学进展，2025，7（1）：29-32.
https://doi.org/10.35534/pss.0701005

何对未在三亚市收集产生的个人数据进行分级分类。这些均是三亚市在处理个人数据跨境流动时需要直视和解决的问题。

（3）安全评估与监管风险

在安全评估方面：①评估流程不规范。由于缺乏统一的评估流程和标准，企业和机构在进行个人数据保护评估时存在差异，使得评估结果难以客观、准确与公正。②评估机制亟待完善。在三亚市个人数据保护评估中，专业的评估机构和人才不足，影响评估工作有序推进。③采取“一事一议”的评估方式，客观存在的过度干预，不可避免地影响个人数据跨境流动的自由与流畅。在监管方面：①《数据出境安全评估办法》聚焦个人数据在国内获得有效的监管，但在境外出现的安全风险并且没有被有效化解，那么再有效的国内监管也会变得没有意义；②监管体系存在明显漏洞。监管主体较为分散，涉及诸如市网信部门、电信主管部门、公安部门、市场监管部门以及金融等，这种多头监管方式，极易出现监管空白、重复监管甚至部门之间相互推诿、扯皮等的情况发生。

2　上海市和广州市在个人数据跨境流动安全风险防控方面的具体做法

（1）上海市的主要做法。在上海自由贸易试验区临港新片区：①巩固电信基础设施。建设国际海底光缆、国际贸易试验数据港；启动促进数据跨境高效流动的“信息飞鱼”。②探索数据跨境安全流动机制。探索数据跨境流动分类监管模式，开展数据跨境传输安全管理试点;支持在集成电路、人工智能等几个重点领域开展数据跨境流动安全评估、备份审查、数据保护能力认证、交易风险评估等数据跨境安全管理机制。③营造开放性数字营商环境。推进并完善了云服务等领域的外资准入和监管政策，致力于打造符合高国际标准的数据产业园区。

2021年11月25日，上海市通过了《上海市数据条例》，该条例建立了全面的数据安全治理体系：一是实行数据安全责任制，确认数据处理者的主体责任和安保义务。二是建立健全数据分类分级保护制度，确定本市重要数据目录，对列入目录的数据进行重点保护。三是明确切分信息化职能整合后市级责任部门和市大数据中心的数据安全责任。四是建立监测预警和应急处置机制，推动数据安全检测评估、认证等服务机构的发展。该条例第六十九条规定，上海市在临港新片区内探索制定低风险跨境流动数据目录，促进数据跨境安全、自由流动。在临港新片区内依法开展跨境数据活动的自然人、法人和非法人组织，应当按照要求报送相关信息。

2024年2月8日，上海市公布《中国（上海）自由贸易试验区临港新片区数据跨境流动分类分级管理办法（试行）》（以下简称《管理办法》），第三章、第四章和第五章分别规定了数据跨境分类分级管理、重要数据目录管理和一般数据清单管理。《管理办法》围绕汽车、金融、航运、生物医药等重点领域，以及临港新片区相关行业的发展要求对跨境数据进行分类管理。将跨境数据分为核心数据、重要数据、一般数据3个级别，并为这三类数据设计不同的跨境规则：核心数据禁止跨境，重要数据通过临港新片区数据跨境服务中心申报数据出境安全评估，一般数据自由跨境流动。此外，《管理办法》还要求临港新片区管委会负责对重要数据目录、一般数据清单进行更新，以及对数据处理者的数据跨境活动进行日常监督检查以及抽查。最后，还结合临港新片区的实际情况对“核心数据”“重要数据”“一般数据”重新进行界定。

（2）广州市的主要做法。2023年7月21日，广州公布了《广州市数据条例（公开征求意见稿）》（以下简称《意见稿》）。该意见稿第三十九条规定，广州市支持南沙在国家数据跨境传输安全管理制度框架下，开展数据跨境流动安全管理试点，建设国际光缆登陆站和国际互联网接入绿色通道，探索开展离岸数据服务试点，构建数据跨境监管模式，探索跨境数据流通“白名单”制度，保障数据跨境安全。除此之外，《意见稿》确立数据安全管理原则，坚持安全和发展并重，建立健全分类分级、风险防范、应急处置等数据安全管理机制，鼓励研发数据安全技术，保障数据全生命周期安全，并实行数据安全主体责任制、建立健全数据分类分级保护制度和数据安全风险评估与监管体系，加强数据要素安全监管治理，保障数据安全。这些措施反映了广州市在数据跨境流动和安全监管方面的前瞻性和创新性，展现了城市在数据安全法律法规建设方面的积极探索，旨在为数据跨境流动提供一个安全、可靠、高效的环境，同时也为促进经济的数字化转型提供了有力的法律支撑。

3　三亚市个人数据跨境流动安全防控的具体对策与建议

在《网络安全法》《网络安全审查办法》《数据安全法》《个人信息保护法》《数据出境安全评估办法》《个人信息出境标准合同办法》和《促进和规范数据跨境流动规定》的指导下，借鉴上海和广州的做法，并结合本地实际情况，在个人数据流动安全方面探索“三亚模式”。建议三亚市在制定《三亚市数据条例》，构建数据安全治理体系时，重点把握以下几个方面。

（1）实行数据安全管理原则，防止个人数据泄露。①数据加密与安全防护：加强对个人数据的加密和安全防护措施，采用先进的加密技术和安全协议，确保个人数据在传输和存储过程中的安全。②限制数据访问权限：严格限制个人数据的访问权限，确保只有经过授权的人员才能访问、处理和使用个人数据，防止未经授权

的数据泄露和滥用。③加强数据主体权益保护：尊重数据主体的知情权、同意权、访问权、更正权、删除权等权益，确保数据主体充分了解个人数据的收集、使用、存储和传输情况，并自主决定是否同意个人数据的跨境传输。④建立数据泄露应急响应机制：建立数据泄露应急响应机制，一旦发生数据泄露事件，能够及时采取响应、处置和报告措施，最大限度地减少数据泄露对个人和社会造成的损失。

（2）建立健全数据分类分级保护机制。首先，借鉴上海市的做法，将个人数据分为三个等级并对其进行重新界定。以对国家安全、个人隐私、个人生命和财产的影响程度为标准，将个人数据分为一般个人数据、敏感个人数据和关键个人数据。其中，一般个人数据包括身高、体重、教育经历等可以为公众所知悉的信息。敏感个人信息包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。关键个人数据表现为财产信息、家庭住址、健康数据等直接影响到个人的财产和生命安全的信息。其次，对“不是在三亚市收集产生的个人信息”采取全面解读，规定为“收集行为及收集主体未在三亚市”，以促进数据的有序跨境流动。这里还应注意两类个人数据：第一类为境外产生和境外收集的个人数据，经三亚市过境中转；第二类为虽在境外产生和境外收集的个人数据但经过三亚市加工处理，在三亚市运营产生的个人数据出境。第一类个人数据可以直接出境，其能成功跨境说明已达到出境方的要求，三亚市只是中转站，因此不需要经过评估和审批；第二类数据即使也为境外产生和境外收集的个人数据，但流入三亚市后，经国内人员引入境内个人信息或者重要数据进行加工处理，已与三亚市产生密切联系，因此需要与三亚市个人信息一样对其进行分类。最后，以国家安全作为前提条件，并以《国家安全法》中的相关规定为模板重构以“自由化为原则、本土化为例外”的个人数据跨境规则，对一般个人数据、敏感个人数据进行有限制的跨境流动，即以“传输为原则、禁止为例外”设定跨境流动规则。关键个人信息只能储存在本市且禁止流动。在国家基本安全得到保障的前提下，最大限度地促进个人数据跨境流动。

（3）建立个人数据跨境流动清单。主要包括正负面清单两类，其中，正面清单记录适格跨境的个人数据和适格的出境目标地两项内容，只要是被记入正面清单中的一般个人数据，流入该清单中的国家和地区时，不需要再履行额外的审批手续，即为个人数据跨境流动打通了一条“绿色通道”。记入正面清单中的个人数据还包括敏感个人数据，相较于一般个人数据而言，敏感个人数据的跨境流动还需要经过一定的审批程序。负面清单为禁止跨境的关键个人数据和不能对个人数据提供充分保护的地区和国家。有下列情形之一的，可以进入正面清单：①与我国签署同一国际协定的成员国，如《区域全面经济伙伴关系协定》（RCEP）。能成为同一份国际规则的成员国一定有着共同的数字经济发展诉求，因此自然能进入正面清单。需要注意的是，有些国际协定的条款并不是一开始就对成员国产生效力的，如RCEP协定规定，柬埔寨、老挝和缅甸在该协定生效之日起五年内不得被要求适用第十二章第八条第一款。因此，为了有效保护三亚市个人数据跨境活动，正面清单中需根据国际协定的规定适当予以调整，具体调整时间以相关国际协定为准。②针对未参与同一个国际协定的国家和地区。三亚市需要对出境目标地的风险（政策法律+安全环境）进行评估，以确保出境目标地的政策法律“有效保障”数据安全。例如，是否存在可以抑制“长臂管辖”的条款、是否有完毕的司法救济措施，以及能否对网络犯罪活动有效制裁等。如果出境目标地能达到我国个人数据保护的最低要求，那么可以进入三亚市正面清单。故正负面清单并非一成不变，可根据我国所加入的国际协定，以及个人数据出境目标地的综合情况予以调整，因而构建周期性评估机制和重新评估机制尤为重要和必要。

（4）建立个人数据安全责任制。从评估环节着手，明确报送主体、相关方的责任以及相应的报送规定：①在处理者与受托处理者之间，数据处理者负责数据出境安全评估申报，受托处理者在职责与约定范围内协助评估。②在共同数据处理者之间，明确“大”数据处理者囊括“小”数据处理者；如果均为“大”数据处理者，各自均需申报。③申报主体尽量使用三亚市主体，且考量主体隔离、所持牌照完备性等因素。从个人信息的主体资质、出境数量、出境质量和出境用途等角度，进行全面兼顾与精准把握；从个人数据跨境流动着手，建议摒弃“一事一议”的安全评估模式，建立基于数据类型的跨境流动规则，借助正面清单简化审批程序，从而促进数据贸易的便利化。在监管模式上，对内，吸纳上海市的做法，设置独立的个人数据监管机构或者指定一个机构专门对数据处理者的数据跨境活动进行日常监督检查以及抽查；对外，借鉴《数字经济伙伴关系协定》（DEPA）规定，将监管贯穿于个人数据跨境流动的全过程。对不同类型的个人数据采用不同的监管模式：对一般个人数据和敏感个人数据，三亚市从出境目标地是否有效执行约定责任义务条款，以及当高敏感数据面临风险时，出境目标地是否采取相关技术或制度措施可以将风险降低到可控范围两方面，监测个人数据流入目标地之后的具体情况；对于关键个人数据坚守事前防范的监管模式。在此基础上，引入问责机制。问责对象为个人数据掌控者，其为个人数据安全责任主体。具体责任形式为：①行政责任。如违反《三亚市数据条例》的规定，依法受到行政处罚的，相关信息纳入本市公共信用信息服务平台，由有关部门依法开展联合惩戒。②违反

https://doi.org/10.35534/pss.0701005

《三亚市数据条例》规定处理个人信息，侵害众多个人的权益的，人民检察院、市消费者权益保护委员会，以及由国家网信部门确定的组织，可以依法向人民法院。此举倒逼个人数据的处理者严于律己，采取合理、合法的措施保障数据安全。

此外，三亚市结合实际，在巩固电信基础设施方面，建设国际海底光缆及登陆点、国际互联网数据交互试点、国际通信入口局。在探索数据跨境安全流动机制方面，探索数据跨境传输安全管理试点；支持在集成电路、人工智能等几个重点领域开展数据跨境流动安全评估、备份审查、数据保护能力认证、交易风险评估等数据跨境安全管理机制。在营造开放性数字营商环境方面，按照省里的部署，逐步开放电信业务市场准入和增值电信的外资股比限制等方面。在机制创新方面，探索更加便利的个人信息安全出境评估颁发。开展个人信息入境制度对接，探索加入区域性国际数据跨境流动制度安排，提升数据传输便利性。

参考文献

[1] 高志宏．个人信息保护的公共利益考量——以应对突发公共卫生事件为视角 [J]．东方法学，2022（3）：17–32.
[2] 吕宁宁，蒋欣．比较视角下的RCEP争端解决机制研究 [J]．国际法学刊，2023（4）：131–154，157–158.
[3] 赵世璐．跨境数据流动的例外规则研究 [D]．华东政法大学，2023.
[4] 魏如连．上海自贸区数据跨境“一般数据清单”的国际数字经贸规则规范性研究 [C]//航运法治保障研究文集．山东大学法学院，2024：8.
[5] 岳树梅，徐昌登．RCEP数据跨境流动的法律障碍与创新策略 [J]．长春大学学报，2024，34（9）：80–85.
[6] 马海桐．RCEP跨境数据流动的规则检视与中国因应 [J]．对外经贸，2024（6）：30–33.

Countermeasures and Suggestions for Security Prevention and Control of Cross-border Flow of Personal Data in Sanya City

Wei Hailang

University of Sanya, Sanya

Abstract: Since the 18th National Congress of the Communist Party of China (CPC), General Secretary Xi Jinping has emphasized in a number of meetings that “national data security must be guaranteed in an effective manner”. With the proliferation of data volumes and the increasing frequency of cross-border data flows, strong data security protection and flow regulation will become an important guarantee of national security. Hainan Province has persistently and thoroughly studied and implemented the spirit of General Secretary Xi Jinping’s important exposition on national data security, and comprehensively coordinated and promoted data security work in various fields. Sanya city has responded positively to national policy and regulatory requirements, stating clearly that in the future the City will pay more attention to “safeguarding national data security and strengthening protection of personal information”. Starting from security prevention and control of cross-border flow of personal data, the article not only analyzes deficiencies in the security prevention and control of cross-border flow of personal data in Sanya City but also puts forward four suggestions to improve security prevention and control measures of cross-border flow of personal data in Sanya City, taking into account experiences and practices of Shanghai and Guangzhou Municipality.

Key words: Personal data; Cross-border data flow; Category and classification of data; Regulation; Assessment